

What is claimed is:

1 1. A reception apparatus which receives and reproduces  
2 scrambled content, comprising:

3 reception means for receiving the scrambled content,  
4 wherein the scrambled content is scrambled so that a  
5 predetermined unit of scrambled content, which is a portion  
6 of the scrambled content, is descrambled using a  
7 descrambling key corresponding to the predetermined unit  
8 of scrambled content, and at least one piece of storage  
9 information in which a list including all descrambling keys  
10 to be used for descrambling the scrambled content is  
11 embedded;

12 storage means for storing the received scrambled  
13 content and the storage information;

14 list extraction means for extracting the list from  
15 the stored storage information;

16 descramble processing means for (a) extracting the  
17 predetermined unit of scrambled content from the stored  
18 scrambled content, (b) extracting a descrambling key  
19 corresponding to the predetermined unit of scrambled  
20 content from the extracted list, and (c) descrambling the  
21 extracted predetermined unit of scrambled content using  
22 the extracted descrambling key; and

23 reproduction means for reproducing the predetermined  
24 unit of descrambled content in the descrambled order.

1 2. The reception apparatus of Claim 1, wherein

2 the reception means receives one piece of storage  
3 information in which the list is embedded,

4 the storage means stores the received scrambled  
5 content and the one piece of storage information, and  
6 the list extraction means extracts the list from the  
7 stored one piece of storage information.

1 3. The reception apparatus of Claim 1, wherein

2 the reception means receives a plurality of pieces  
3 of storage information in each piece of which a divided  
4 portion of the list is embedded,

5 the storage means stores the received scrambled  
6 content and the plurality of pieces of storage information,  
7 and

8 the list extraction means extracts the list from the  
9 stored plurality of pieces of storage information.

1 4. The reception apparatus of Claim 1, wherein

2 the reception means sequentially receives a  
3 transport stream (TS) packet including the predetermined  
4 unit of scrambled content,

5 the storage means sequentially stores the received  
6 TS packet, wherein

7 the descramble processing means includes:

8 scrambled content extraction means for extracting  
9 the predetermined unit of scrambled content from one of  
10 the TS packets stored in the storage means, and counting

11 the ordinal position of the TS packet from the leading TS  
12 packet;

13 descrambling key extraction means for extracting a  
14 descrambling key from the list, based on the counted  
15 ordinal position; and

16 descrambling means for descrambling the extracted  
17 predetermined unit of scrambled content using the  
18 extracted descrambling key.

1 5. The reception apparatus of Claim 1, wherein  
2 the reception means receives at least one storage  
3 Entitlement Control Message (ECM) as the at least one piece  
4 of storage information, the list being embedded in a  
5 portion to be encoded in the main body of the ECM,  
6 the storage means stores the received storage ECMs,  
7 and  
8 the list extraction means interprets the stored  
9 storage ECMs to extract the list.

1 6. The reception apparatus of Claim 5, wherein  
2 the reception means receives the storage ECMs  
3 including identifying information for distinguishing the  
4 storage ECMs from another type of ECM.

1 7. The reception apparatus of Claim 5, wherein  
2 the reception means receives the storage ECMs at a  
3 time.

1 8. The reception apparatus of Claim 1, wherein  
2 the reception means sequentially receives a TS packet  
3 including (a) the predetermined unit of scrambled content  
4 and (b) packet specifying information for specifying an  
5 unscrambled TS packet, and  
6 the storage means sequentially stores the received  
7 TS packet, wherein  
8 the descramble processing means includes:  
9 scrambled content extraction means for extracting  
10 the predetermined unit of scrambled content and the packet  
11 specifying information from one of the TS packets stored  
12 in the storage means;  
13 descrambling key extraction means for extracting a  
14 descrambling key from the list, based on the extracted  
15 packet specifying information; and  
16 descrambling means for descrambling the extracted  
17 predetermined unit of scrambled content using the  
18 extracted descrambling key.

1 9. The reception apparatus of Claim 8, wherein  
2 the packet specifying information is one of  
3 Continuity Counter (CC), the number of TS packets, a  
4 cumulative amount of data, a relative reproduction time,  
5 and a scrambling key identifier,  
6 the scrambled content extraction means extracts, as  
7 the packet specifying information, one of the Continuity

8 Counter (CC), the number of TS packets, the cumulative  
9 amount of data, the relative reproduction time, and the  
10 scrambling key identifier, and

11 the descrambling key extraction means performs a  
12 predetermined operation to the extracted information as  
13 the packet identifying information to generate a  
14 descrambling key identifier, and extracts a descrambling  
15 key from the list based on the descrambling key identifier.

1 10. The reception apparatus of Claim 1, wherein

2 the reception means sequentially receives a TS packet  
3 including (a) the predetermined unit of scrambled content  
4 and (b) unscrambled I picture information, wherein the I  
5 picture information indicates whether the TS packet  
6 corresponding to the information consists of a portion of  
7 an I picture/an I picture or not, and

8 the storage means sequentially stores the received  
9 TS packet, wherein

10 the descramble processing means includes:

11 scrambled content extraction means for, when  
12 performing particular reproduction processes, extracting  
13 the predetermined unit of scrambled content and I picture  
14 information from one of the TS packets stored in the storage  
15 means;

16 I picture judgement means for judging whether the  
17 extracted predetermined unit of scrambled content consists  
18 of a portion of an I picture/an I picture or not, based

19 on the extracted I picture information;  
20 descrambling key extraction means for extracting a  
21 descrambling key from the list, only when the extracted  
22 predetermined unit of scrambled content consists of a  
23 portion of an I picture/an I picture; and  
24 descrambling means for descrambling the extracted  
25 predetermined unit of scrambled content using the  
26 extracted descrambling key.

1 11. The reception apparatus of Claim 1 further managing  
2 contract information and consisting of a security module  
3 whose portion does not effectively function if a contract  
4 has not been made, and other modules, the reception  
5 apparatus further comprising:

6 list holding means for holding the list extracted by  
7 the list extraction means,

8 wherein the list extraction means and the list  
9 holding means are provided within the security module.

1 12. A reception apparatus which receives and reproduces  
2 scrambled content, comprising:

3 reception means for receiving the scrambled content,  
4 wherein the scrambled content is scrambled so that a  
5 predetermined unit of scrambled content, which is a portion  
6 of the scrambled content, is descrambled using a  
7 descrambling key corresponding to the predetermined unit  
8 of scrambled content, and a descrambling key is attached

9 to each predetermined unit of scrambled content;  
10 storage means for storing the received scrambled  
11 content;  
12 list generation means for, when/after storing the  
13 received scrambled content by the storage means,  
14 generating a list including all descrambling keys to be  
15 used for descrambling the scrambled content, based on the  
16 descrambling key attached to each predetermined unit of  
17 scrambled content;  
18 descramble processing means for (a) extracting the  
19 predetermined unit of scrambled content from the stored  
20 scrambled content, (b) extracting a descrambling key  
21 corresponding to the extracted predetermined unit of  
22 scrambled content from the generated list, and (c)  
23 descrambling the extracted predetermined unit of scrambled  
24 content using the extracted descrambling key; and  
25 reproduction means for reproducing the predetermined  
26 unit of descrambled content in the descrambled order.

1 13. The reception apparatus of Claim 12, wherein  
2 the reception means sequentially receives a TS packet  
3 including (a) the predetermined unit of scrambled content,  
4 and (b) auxiliary information including a descrambling key  
5 and information for associating the descrambling key with  
6 scrambled content,  
7 the storage means sequentially stores the received  
8 TS packet, and

9           the list generation means generates the list, based  
10 on the auxiliary information.

1   14.   The reception apparatus of Claim 13, wherein  
2           the TS packet includes an ECM, the auxiliary  
3 information being embedded in a portion to be encoded in  
4 a main body of the ECM, and

5           the list generation means extracts the auxiliary  
6 information embedded in the ECM, and generates the list  
7 based on the auxiliary information.

1   15.   A broadcast apparatus which scrambles content and  
2 broadcasts the scrambled content to a reception apparatus,  
3 the broadcast apparatus comprising:

4           acquisition means for acquiring content to be  
5 scrambled and a plurality of descrambling keys;

6           scramble processing means for scrambling a  
7 predetermined unit of content out of the acquired content  
8 so that the predetermined unit of scrambled content is  
9 descrambled using a descrambling key different for each  
10 predetermined unit or each set of a plurality of  
11 predetermined units;

12          attaching means for attaching auxiliary information  
13 to the predetermined unit of scrambled content, the  
14 auxiliary information consisting of (a) information for  
15 identifying the scrambled content and (b) a descrambling  
16 key corresponding to the content, and used for having the



17 reception apparatus generate a list of the descrambling  
18 keys; and

19 broadcast means for broadcasting the scrambled  
20 content to which the auxiliary information is added.

1 16. The broadcast apparatus of Claim 15, wherein  
2 the attaching means embeds the auxiliary information  
3 in a portion to be encoded in a main body of an ECM and  
4 attaches the ECM to the predetermined unit of scrambled  
5 content.

1 17. A broadcast apparatus which scrambles content and  
2 broadcasts the scrambled content to a reception apparatus,  
3 the broadcast apparatus comprising:

4 acquisition means for acquiring content to be  
5 scrambled and a plurality of descrambling keys;

6 list generation means for generating a list of the  
7 descrambling keys;

8 embedding means for embedding the list in at least  
9 one piece of predetermined information to generate at least  
10 one piece of storage information;

11 scramble processing means for scrambling a  
12 predetermined unit of content out of the acquired content  
13 so that the predetermined unit of scrambled content is  
14 descrambled using a descrambling key different for each  
15 predetermined unit or each set of a plurality of  
16 predetermined units; and

17 broadcast means for broadcasting the generated  
18 storage information and the scrambled content.

1 18. The broadcast apparatus of Claim 17, wherein  
2 the embedding means embeds the list in one piece of  
3 predetermined information to generate one piece of storage  
4 information, and  
5 the broadcasting means broadcasts the generated one  
6 piece of information and the scrambled content.

1 19. The broadcast apparatus of Claim 17, wherein  
2 the embedding means embeds a divided portion of the  
3 list in each of a plurality of pieces of predetermined  
4 information to generate a plurality of pieces of storage  
5 information, and  
6 the broadcasting means broadcasts the generated  
7 plurality of pieces of storage information and the  
8 scrambled content.

1 20. The broadcast apparatus of Claim 17, wherein  
2 the embedding means embeds the list in a portion to  
3 be encoded in a main body of at least one ECM to generate  
4 at least one piece of storage information.

1 21. The broadcast apparatus of Claim 17, wherein  
2 the broadcast means broadcasts one set of the storage  
3 information while all the scrambled content corresponding

4 to the storage information are broadcast once.

1 22. A program used for a reception apparatus which  
2 receives and reproduces scrambled content, the program has  
3 the reception apparatus conduct the following steps of:

4 a reception step for receiving the scrambled content,  
5 wherein the scrambled content is scrambled so that a  
6 predetermined unit of scrambled content, which is a portion  
7 of the scrambled content, is descrambled using a  
8 descrambling key corresponding to the predetermined unit  
9 of scrambled content, and at least one piece of storage  
10 information in which a list including all descrambling keys  
11 to be used for descrambling the scrambled content is  
12 embedded;

13 a storage step for storing the received scrambled  
14 content and the storage information;

15 a list extraction step for extracting the list from  
16 the stored storage information;

17 a descramble processing step for (a) extracting the  
18 predetermined unit of scrambled content from the stored  
19 scrambled content, (b) extracting a descrambling key  
20 corresponding to the predetermined unit of scrambled  
21 content from the extracted list, and (c) descrambling the  
22 extracted predetermined unit of scrambled content using  
23 the extracted descrambling key; and

24 a reproduction step for reproducing the  
25 predetermined unit of descrambled content in the

26 descrambled order.

1 23. A program used for a reception apparatus which  
2 receives and reproduces scrambled content, the program has  
3 the reception apparatus conduct the following steps of:  
4 a reception step for receiving the scrambled content,  
5 wherein the scrambled content is scrambled so that a  
6 predetermined unit of scrambled content, which is a portion  
7 of the scrambled content, is descrambled using a  
8 descrambling key corresponding to the predetermined unit  
9 of scrambled content, and a descrambling key is attached  
10 to each predetermined unit of scrambled content;  
11 a storage step for storing the received scrambled  
12 content;  
13 a list generation step for, when/after storing the  
14 received scrambled content in the storage step, generating  
15 a list including all descrambling keys to be used for  
16 descrambling the scrambled content, based on the  
17 descrambling key attached to each predetermined unit of  
18 scrambled content;  
19 a descramble processing step for (a) extracting the  
20 predetermined unit of scrambled content from the stored  
21 scrambled content, (b) extracting a descrambling key  
22 corresponding to the extracted predetermined unit of  
23 scrambled content from the generated list, and (c)  
24 descrambling the extracted predetermined unit of scrambled  
25 content using the extracted descrambling key; and

26           a reproduction step for reproducing the  
27 predetermined unit of descrambled content in the  
28 descrambled order.

1   24.   A program used for a broadcast apparatus which  
2   scrambles content and broadcasts the scrambled content to  
3   a reception apparatus, the program has the broadcast  
4   apparatus conduct the following steps of:

5           an acquisition step for acquiring content to be  
6   scrambled and a plurality of descrambling keys;

7           a scramble processing step for scrambling a  
8   predetermined unit of content out of the acquired content  
9   so that the predetermined unit of scrambled content is  
10   descrambled using a descrambling key different for each  
11   predetermined unit or each set of a plurality of  
12   predetermined units;

13          an attaching step for attaching auxiliary  
14   information to the predetermined unit of scrambled content,  
15   the auxiliary information consisting of (a) information  
16   for identifying the scrambled content and (b) a  
17   descrambling key corresponding to the content, and used  
18   for having the reception apparatus generate a list of the  
19   descrambling keys; and

20          a broadcast step for broadcasting the scrambled  
21   content to which the auxiliary information is added.

1   25.   A program used for a broadcast apparatus which

2 scrambles content and broadcasts the scrambled content to  
3 a reception apparatus, the program has the broadcast  
4 apparatus conduct the following steps of:

5 an acquisition step for acquiring content to be  
6 scrambled and a plurality of descrambling keys;

7 a list generation step for generating a list of the  
8 descrambling keys;

9 an embedding step for embedding the list in at least  
10 one piece of predetermined information to generate at least  
11 one piece of storage information;

12 a scramble processing step for scrambling a  
13 predetermined unit of content out of the acquired content  
14 so that the predetermined unit of scrambled content is  
15 descrambled using a descrambling key different for each  
16 predetermined unit or each set of a plurality of  
17 predetermined units; and

18 a broadcast step for broadcasting the generated  
19 storage information and the scrambled content.

1 26. A recording medium on which a program used for a  
2 reception apparatus which receives and reproduces  
3 scrambled content is recorded, the program has the  
4 reception apparatus conduct the following steps of:

5 a reception step for receiving the scrambled content,  
6 wherein the scrambled content is scrambled so that a  
7 predetermined unit of scrambled content, which is a portion  
8 of the scrambled content, is descrambled using a

9 descrambling key corresponding to the predetermined unit  
10 of scrambled content, and at least one piece of storage  
11 information in which a list including all descrambling keys  
12 to be used for descrambling the scrambled content is  
13 embedded;

14 a storage step for storing the received scrambled  
15 content and the storage information;

16 a list extraction step for extracting the list from  
17 the stored storage information;

18 a descramble processing step for (a) extracting the  
19 predetermined unit of scrambled content from the stored  
20 scrambled content, (b) extracting a descrambling key  
21 corresponding to the predetermined unit of scrambled  
22 content from the extracted list, and (c) descrambling the  
23 extracted predetermined unit of scrambled content using  
24 the extracted descrambling key; and

25 a reproduction step for reproducing the  
26 predetermined unit of descrambled content in the  
27 descrambled order.

1 27. A recording medium on which a program used for a  
2 reception apparatus which receives and reproduces  
3 scrambled content is recorded, the program has the  
4 reception apparatus conduct the following steps of:

5 a reception step for receiving the scrambled content,  
6 wherein the scrambled content is scrambled so that a  
7 predetermined unit of scrambled content, which is a portion

8 of the scrambled content, is descrambled using a  
9 descrambling key corresponding to the predetermined unit  
10 of scrambled content, and a descrambling key is attached  
11 to each predetermined unit of scrambled content;

12 a storage step for storing the received scrambled  
13 content;

14 a list generation step for, when/after storing the  
15 received scrambled content in the storage step, generating  
16 a list including all descrambling keys to be used for  
17 descrambling the scrambled content, based on the  
18 descrambling key attached to each predetermined unit of  
19 scrambled content;

20 a descramble processing step for (a) extracting the  
21 predetermined unit of scrambled content from the stored  
22 scrambled content, (b) extracting a descrambling key  
23 corresponding to the extracted predetermined unit of  
24 scrambled content from the generated list, and (c)  
25 descrambling the extracted predetermined unit of scrambled  
26 content using the extracted descrambling key; and

27 a reproduction step for reproducing the  
28 predetermined unit of descrambled content in the  
29 descrambled order.

1 28. A recording medium on which a program used for a  
2 broadcast apparatus which scrambles content and broadcasts  
3 the content to a reception apparatus is recorded, the  
4 program has the broadcast apparatus conduct the following



5 steps of:

6 an acquisition step for acquiring content to be  
7 scrambled and a plurality of descrambling keys;

8 a scramble processing step for scrambling a  
9 predetermined unit of content out of the acquired content  
10 so that the predetermined unit of scrambled content is  
11 descrambled using a descrambling key different for each  
12 predetermined unit or each set of a plurality of  
13 predetermined units;

14 an attaching step for attaching auxiliary  
15 information to the predetermined unit of scrambled content,  
16 the auxiliary information consisting of (a) information  
17 for identifying the scrambled content and (b) a  
18 descrambling key corresponding to the content, and used  
19 for having the reception apparatus generate a list of the  
20 descrambling keys; and

21 a broadcast step for broadcasting the scrambled  
22 content to which the auxiliary information is added.

1 29. A recording medium on which a program used for a  
2 broadcast apparatus which scrambles content and broadcasts  
3 the content to a reception apparatus is recorded, the  
4 program has the broadcast apparatus conduct the following  
5 steps of:

6 an acquisition step for acquiring content to be  
7 scrambled and a plurality of descrambling keys;

8 a list generation step for generating a list of the

9        descrambling keys;  
10            an embedding step for embedding the list in at least  
11        one piece of predetermined information to generate at least  
12        one piece of storage information;  
13            a scramble processing step for scrambling a  
14        predetermined unit of content out of the acquired content  
15        so that the predetermined unit of scrambled content is  
16        descrambled using a descrambling key different for each  
17        predetermined unit or each set of a plurality of  
18        predetermined units; and  
19            a broadcast step for broadcasting the generated  
20        storage information and the scrambled content.

1        30.    A computer-readable recording medium on which  
2        content to be broadcast to a reception apparatus is  
3        recorded, wherein the reception apparatus receives and  
4        stores scrambled content, and descrambles and reproduces  
5        the stored scrambled content, the content comprising:  
6            scrambled content which is scrambled so that a  
7        predetermined unit of scrambled content, which is a portion  
8        of the scrambled content, is descrambled using a  
9        descrambling key corresponding to the predetermined unit  
10       of content, and  
11            a storage ECM, wherein a list including all  
12       descrambling keys used for descrambling the scrambled  
13       content is embedded in a portion to be encoded in a main  
14       body of at least one ECM.

1 31. A method for receiving and reproducing scrambled  
2 content, the method comprising the steps of:  
3 a reception step for receiving the scrambled content,  
4 wherein the scrambled content is scrambled so that a  
5 predetermined unit of scrambled content, which is a portion  
6 of the scrambled content, is descrambled using a  
7 descrambling key corresponding to the predetermined unit  
8 of scrambled content, and at least one piece of storage  
9 information in which a list including all descrambling keys  
10 to be used for descrambling the scrambled content is  
11 embedded;  
12 a storage step for storing the received scrambled  
13 content and the storage information;  
14 a list extraction step for extracting the list from  
15 the stored storage information;  
16 a descramble processing step for (a) extracting the  
17 predetermined unit of scrambled content from the stored  
18 scrambled content, (b) extracting a descrambling key  
19 corresponding to the predetermined unit of scrambled  
20 content from the extracted list, and (c) descrambling the  
21 extracted predetermined unit of scrambled content using  
22 the extracted descrambling key; and  
23 a reproduction step for reproducing the  
24 predetermined unit of descrambled content in the  
25 descrambled order.

1 32. A method for receiving and reproducing scrambled  
2 content, the method comprising the steps of:  
3 a reception step for receiving the scrambled content,  
4 wherein the scrambled content is scrambled so that a  
5 predetermined unit of scrambled content, which is a portion  
6 of the scrambled content, is descrambled using a  
7 descrambling key corresponding to the predetermined unit  
8 of scrambled content, and a descrambling key is attached  
9 to each predetermined unit of scrambled content;  
10 a storage step for storing the received scrambled  
11 content;  
12 a list generation step for, when/after storing the  
13 received scrambled content in the storage step, generating  
14 a list including all descrambling keys to be used for  
15 descrambling the scrambled content, based on the  
16 descrambling key attached to each predetermined unit of  
17 scrambled content;  
18 a descramble processing step for (a) extracting the  
19 predetermined unit of scrambled content from the stored  
20 scrambled content, (b) extracting a descrambling key  
21 corresponding to the extracted predetermined unit of  
22 scrambled content from the generated list, and (c)  
23 descrambling the extracted predetermined unit of scrambled  
24 content using the extracted descrambling key; and  
25 a reproduction step for reproducing the  
26 predetermined unit of descrambled content in the  
27 descrambled order.

1 33. A method for scrambling content and broadcasting the  
2 scrambled content to a reception apparatus, the method  
3 comprising the steps of:

4 an acquisition step for acquiring content to be  
5 scrambled and a plurality of descrambling keys;

6 a scramble processing step for scrambling a  
7 predetermined unit of content out of the acquired content  
8 so that the predetermined unit of scrambled content is  
9 descrambled using a descrambling key different for each  
10 predetermined unit or each set of a plurality of  
11 predetermined units;

12 an attaching step for attaching auxiliary  
13 information to the predetermined unit of scrambled content,  
14 the auxiliary information consisting of (a) information  
15 for identifying the scrambled content and (b) a  
16 descrambling key corresponding to the content, and used  
17 for having the reception apparatus generate a list of the  
18 descrambling keys; and

19 a broadcast step for broadcasting the scrambled  
20 content to which the auxiliary information is added.

1 34. A method for scrambling content and broadcasting the  
2 scrambled content to a reception apparatus, the method  
3 comprising the steps of:

4 an acquisition step for acquiring content to be  
5 scrambled and a plurality of descrambling keys;

6           a list generation step for generating a list of the  
7   descrambling keys;  
8           an embedding step for embedding the list in at least  
9   one piece of predetermined information to generate at least  
10   one piece of storage information;  
11          a scramble processing step for scrambling a  
12   predetermined unit of content out of the acquired content  
13   so that the predetermined unit of scrambled content is  
14   descrambled using a descrambling key different for each  
15   predetermined unit or each set of a plurality of  
16   predetermined units; and  
17          a broadcast step for broadcasting the generated  
18   storage information and the scrambled content.